

Oracle® Fusion Cloud EPM

Amministrazione del controllo dell'accesso per
Oracle Enterprise Performance Management
Cloud



F28914-21



Oracle Fusion Cloud EPM Amministrazione del controllo dell'accesso per Oracle Enterprise Performance Management Cloud,

F28914-21

Copyright © 2015-, 2024, , Oracle e/o relative consociate.

Autore principale: EPM Information Development Team

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Sommario

Accesso facilitato alla documentazione

Feedback relativi alla documentazione

1 Panoramica di Controllo accesso

Informazioni su questa guida	1-1
Apertura di Controllo accesso	1-2
Gestione di gruppi	1-2
Creazione di gruppi	1-3
Modifica di gruppi	1-4
Eliminazione di gruppi	1-5
Esportazione di gruppi EPM Cloud in un file CSV	1-5
Importazione delle assegnazioni di utenti a un gruppo da un file	1-6
Assegnazione di un utente a molti gruppi	1-7
Utilizzo della ricerca	1-8

2 Gestione dell'assegnazione dei ruoli a livello di applicazione

Panoramica dell'assegnazione dei ruoli applicazione	2-1
Account Reconciliation	2-3
Ruoli applicazione	2-3
Mapping dei ruoli predefiniti	2-6
Enterprise Profitability and Cost Management	2-7
Ruoli applicazione	2-7
Mapping dei ruoli predefiniti	2-9
Planning, FreeForm, Financial Consolidation and Close e Tax Reporting	2-11
Ruoli della piattaforma EPM Cloud	2-11
Ruoli di Integrazione dati	2-13
Ruoli correlati al giornale di consolidamento	2-13
Ruoli Task Manager	2-14
Mapping dei ruoli predefiniti	2-15

Profitability and Cost Management	2-16
Ruoli applicazione	2-16
Mapping dei ruoli predefiniti	2-16
Oracle Enterprise Data Management Cloud ed Enterprise Data Management	2-16
Ruoli applicazione	2-16
Mapping dei ruoli predefiniti	2-17
Assegnazione di ruoli applicazione a un gruppo o a un utente	2-17
Rimozione di ruoli a livello di applicazione assegnati a un gruppo o a un utente	2-19

3 Generazione di report

Generazione di un Report assegnazioni ruoli per un utente o un gruppo	3-1
Visualizzazione del Report assegnazioni ruoli per l'ambiente	3-2
Visualizzazione del Report accesso utenti	3-3
Visualizzazione ed esportazione del Report gruppo utenti	3-4

Accesso facilitato alla documentazione

Per informazioni sull'impegno di Oracle riguardo l'accesso facilitato, visitare il sito Web Oracle Accessibility Program all'indirizzo <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Accesso al Supporto Oracle

I clienti Oracle che hanno acquistato il servizio di supporto tecnico hanno accesso al supporto elettronico attraverso My Oracle Support. Per informazioni, visitare <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> oppure <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> per clienti non utenti.

Feedback relativi alla documentazione

Per fornire un feedback su questa documentazione, fare clic sul pulsante Feedback in fondo alla pagina in un qualsiasi argomento di Oracle Help Center. È inoltre possibile inviare un messaggio e-mail all'indirizzo epmdoc_ww@oracle.com.

1

Panoramica di Controllo accesso

L'accesso ai componenti di Oracle Enterprise Performance Management Cloud è controllato dai ruoli predefiniti nel dominio di Identity al quale sono assegnati gli utenti. Gli amministratori dei servizi o gli utenti con ruolo applicazione Controllo accesso - Gestisci possono assegnare agli utenti ruoli specifici per le applicazioni Planning, Consolidation, Account Reconciliation e Data Management per consentire loro di eseguire task aggiuntivi in un ambiente.

Ad esempio, gli amministratori servizi possono assegnare a un utente il ruolo di Amministratore approvazioni di un'applicazione Planning o Consolidation per consentire all'utente di svolgere attività correlate alle approvazioni.

Inoltre, gli utenti con ruolo Amministratore servizi possono utilizzare Controllo accesso per creare gruppi composti da utenti o da altri gruppi del dominio di Identity. L'assegnazione di ruoli a questi gruppi consente agli amministratori servizi di concedere i ruoli a più utenti contemporaneamente, riducendo di conseguenza i costi amministrativi.

L'assegnazione di ruoli a livello di applicazione consente di migliorare solo i diritti di accesso degli utenti. Nessuno dei privilegi concessi da un ruolo predefinito può essere ridimensionato da ruoli assegnati a livello di applicazione.

Controllo accesso consente di completare le seguenti attività in un ambiente.

- [Gestione di gruppi](#)
- [Assegnazione di ruoli applicazione a un gruppo o a un utente](#)
- [Generazione di un Report assegnazioni ruoli per un utente o un gruppo](#)
- [Visualizzazione del Report assegnazioni ruoli per l'ambiente](#)
- [Visualizzazione del Report accesso utenti](#)

Collegamento Esercitazione

È inoltre possibile seguire l'esercitazione [Impostazione della sicurezza nei processi aziendali di EPM Cloud](#) per conoscere i livelli di sicurezza nei processi aziendali di EPM Cloud e come gestire la sicurezza con Controllo accesso e le autorizzazioni di accesso.

Informazioni su questa guida

Controllo accesso si applica ai processi aziendali di Oracle Enterprise Performance Management Cloud elencati di seguito.


- Planning
- Planning Modules
- FreeForm
- Consolidamento finanziario e chiusura
- Tax Reporting
- Profitability and Cost Management

- Enterprise Profitability and Cost Management
- Account Reconciliation
- Oracle Enterprise Data Management Cloud
- Narrative Reporting
- Workforce Planning strategico
- Sales Planning

Apertura di Controllo accesso

Per l'assegnazione dei ruoli specifici di applicazione a gruppi e utenti, si utilizza **Controllo accesso**, disponibile nella scheda **Strumenti** della home page.

Per aprire Controllo accesso, procedere come segue.

1. Accedere all'ambiente come amministratore servizi o utente con ruolo applicazione Controllo accesso - Gestisci.
2. Eseguire uno dei passi indicati di seguito.
 - Fare clic su  (Navigator), quindi su **Controllo accesso**.
 - Fare clic su **Strumenti** e quindi su **Controllo accesso**.
 - **Solo per Narrative Reporting**; fare clic su **Controllo accesso**.

Gestione di gruppi

Oracle Enterprise Performance Management Cloud utilizza un repository interno per supportare le assegnazioni di ruoli a livello di applicazione e memorizzare le informazioni nei gruppi di EPM Cloud utilizzati durante il processo di assegnazione dei ruoli.

Gli utenti di EPM Cloud e gli altri gruppi utenti possono essere membri di gruppi gestiti tramite Controllo accesso. È possibile concedere ruoli applicazione agli utenti mediante l'assegnazione di un ruolo al gruppo.

Per consentire la visualizzazione delle assegnazioni utente, in Controllo accesso i ruoli predefiniti sono elencati come gruppi. Non è possibile assegnare loro ruoli o modificarne i ruoli da Controllo accesso. Inoltre, gli utenti EPM Cloud assegnati a ruoli predefiniti sono elencati in Controllo accesso in modo da poter essere aggiunti come membri di gruppo. Fare riferimento alla sezione Introduzione ai ruoli predefiniti in *Guida introduttiva a Oracle Enterprise Performance Management Cloud per gli amministratori*.

In **Gestione gruppi**, i gruppi sono per impostazione predefinita ordinati in base ai valori **Nome gruppo**. Per cercare un gruppo specifico, fare riferimento alla sezione [Utilizzo della ricerca](#) per le istruzioni.

È possibile gestire i gruppi eseguendo le operazioni sotto riportate.

- [Creazione di gruppi](#)
- [Modifica di gruppi](#)
- [Eliminazione di gruppi](#)

- [Esportazione di gruppi EPM Cloud in un file CSV](#)



Nota:

Non è possibile utilizzare Controllo accesso per importare informazioni sui gruppi da un file allo scopo di creare dei gruppi. Per importare i gruppi è possibile utilizzare Migrazione o il comando createGroups di EPM Automate.

Risoluzione dei problemi

Fare riferimento alla sezione Risoluzione dei problemi di gestione utenti, ruoli e gruppi nella *Guida operativa di Oracle Enterprise Performance Management Cloud*.

Creazione di gruppi

Gli amministratori dei servizi o gli utenti con ruolo applicazione Controllo accesso - Gestisci possono creare e gestire i gruppi. Gli utenti di Oracle Enterprise Performance Management Cloud e altri gruppi possono essere membri di un gruppo.



Nota:

È inoltre possibile utilizzare Migrazione o il comando createGroups di EPM Automate per importare da un file le informazioni sui gruppi allo scopo di creare gruppi.

Per creare i gruppi, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento alla sezione [Apertura di Controllo accesso](#).
2. In **Gestione gruppi**, fare clic su **Crea**.
3. In **Crea gruppo**, procedere come segue.
 - a. Nel campo **Nome** immettere un nome di gruppo (massimo 256 caratteri). Per i nomi gruppo non è prevista la distinzione tra maiuscole e minuscole.

EPM Cloud non consente di creare gruppi con nomi identici a nomi di ruoli predefiniti (Amministratore servizi, Utente avanzato, Utente o Responsabile pianificazione e visualizzatore).
 - b. **Facoltativo:** immettere una descrizione del gruppo.
4. **Facoltativo:** aggiungere gruppi per creare un gruppo nidificato.
 - a. In **Gruppi disponibili**, cercare i gruppi. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).

Vengono elencati i gruppi che soddisfano i criteri di ricerca. Per impostazione predefinita, questo elenco è ordinato in base ai valori **Nome gruppo**.
 - b. In **Gruppi disponibili**, selezionare i gruppi membri del nuovo gruppo.
 - c. Fare clic su **Sposta**.

I gruppi selezionati sono riportati in **Gruppi assegnati**. Per rimuovere i gruppi assegnati, selezionare il gruppo da rimuovere in **Gruppi assegnati**, quindi fare clic su **Rimuovi**.

5. **Facoltativo:** aggiungere gli utenti EPM Cloud come membri del gruppo.
Possono essere aggiunti come membri di un gruppo solo gli utenti assegnati a un ruolo predefinito.
 - a. Fare clic su **Utenti**.
 - b. Cercare gli utenti in **Utenti disponibili**. Per istruzioni, fare riferimento alla sezione [Utilizzo della ricerca](#).
Vengono elencati gli utenti che soddisfano i criteri di ricerca. Per impostazione predefinita, questo elenco è ordinato in base ai valori **Login utente**.
 - c. In **Utenti disponibili**, selezionare gli utenti da aggiungere al gruppo.
 - d. Fare clic su **Sposta**.
6. Fare clic su **Salva**.
7. Fare clic su **OK**.

Modifica di gruppi

Gli amministratori dei servizi o gli utenti con ruolo applicazione Controllo accesso - Gestisci possono modificare le proprietà del gruppo, incluso il nome. L'eventuale modifica del nome di un gruppo non ha alcuna conseguenza sui ruoli applicazione assegnati al gruppo né su altre assegnazioni di sicurezza.


Per modificare i gruppi, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
2. **Facoltativo:** in **Gestisci gruppi**, individuare il gruppo da modificare. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).

Vengono elencati i gruppi che soddisfano i criteri di ricerca. Per impostazione predefinita, questo elenco è ordinato in base ai valori **Nome gruppo**.

Nota:

I nomi dei gruppi possono contenere al massimo 256 caratteri. I caratteri visibili, ad esempio, nella colonna **Gruppi disponibili**, potrebbero essere troncati in base alla risoluzione dello schermo.

3. Fare clic su  (Azione) nella riga del gruppo da modificare, quindi selezionare **Modifica**.
4. **Facoltativo:** modificare il nome del gruppo. La modifica del nome del gruppo non ha alcun impatto sulle assegnazioni di sicurezza effettuate mediante il gruppo.
5. Modificare l'assegnazione dei gruppi.
 - a. **Facoltativo:** aggiungere gruppi nidificati.
 - In **Gruppi disponibili**, cercare i gruppi. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
Vengono elencati i gruppi che soddisfano i criteri di ricerca. Per impostazione predefinita, questo elenco è ordinato in base ai valori **Nome gruppo**.

- In **Gruppi disponibili**, selezionare i gruppi e fare clic su **Sposta**.
I gruppi selezionati sono elencati in **Gruppi assegnati**.
- b. **Facoltativo**: rimuovere i gruppi nidificati.
 - In **Gruppi assegnati**, selezionare il gruppo da rimuovere.
 - Fare clic su **Rimuovi**.
- 6. Modificare l'assegnazione degli utenti.
 - a. Fare clic su **Utenti**.
 - b. **Facoltativo**: aggiungere utenti al gruppo.
 - In **Utenti disponibili** cercare gli utenti che si possono assegnare come membri del gruppo. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).


Vengono elencati gli utenti che soddisfano i criteri di ricerca. Per impostazione predefinita, questo elenco è ordinato in base ai valori **Login utente**.
 - In **Utenti disponibili**, selezionare gli utenti e fare clic su **Sposta**.
Gli utenti selezionati sono riportati nell'elenco **Utenti assegnati**.
 - c. **Facoltativo**: rimuovere utenti dal gruppo.
 - In **Utenti assegnati**, selezionare l'utente da rimuovere.
 - Fare clic su **Rimuovi**.
- 7. Fare clic su **Salva**.
- 8. Fare clic su **OK**.

Eliminazione di gruppi

Gli amministratori dei servizi o gli utenti con ruolo applicazione Controllo accesso - Gestisci possono eliminare i gruppi. L'eliminazione di un gruppo non comporta l'eliminazione dei membri che ne fanno parte.

Per eliminare un gruppo, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
2. **Facoltativo**: in **Gestisci gruppi**, cercare il gruppo da eliminare. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).

Vengono elencati i gruppi che soddisfano i criteri di ricerca. Per impostazione predefinita, questo elenco è ordinato in base ai valori **Nome gruppo**.
3. Fare clic su  (Azione) nella riga del gruppo da eliminare, quindi selezionare **Elimina**.
4. Fare clic su **Sì** per confermare l'eliminazione.
5. Fare clic su **OK**.

Esportazione di gruppi EPM Cloud in un file CSV

Gli amministratori dei servizi o gli utenti con ruolo applicazione Controllo accesso - Gestisci possono esportare il nome e le descrizioni dei gruppi di Oracle Enterprise Performance

Management Cloud nel file `Groups.csv` utilizzando **Esporta in formato CSV**. I gruppi predefiniti non vengono esportati.

La voce **Esporta in formato CSV** è disabilitata se non sono presenti gruppi EPM Cloud. TPer utilizzare questa opzione, deve essere presente almeno un gruppo EPM Cloud in Controllo accesso.

1. Aprire **Controllo accesso**. Fare riferimento alla sezione [Apertura di Controllo accesso](#).
La scheda **Gestisci gruppi** elenca tutti i gruppi disponibili.
2. Fare clic su **Esporta in formato CSV** per esportare tutti i gruppi EPM Cloud.
3. Seguire le istruzioni sullo schermo per aprire o salvare il file `Groups.csv`.

Importazione delle assegnazioni di utenti a un gruppo da un file

Gli amministratori dei servizi o gli utenti con ruolo applicazione Controllo accesso - Gestisci possono importare le assegnazioni di utenti a un gruppo da un file con valori separati da virgole (CSV) per creare nuove assegnazioni in un gruppo Controllo accesso esistente. Oracle Enterprise Performance Management Cloud applica le assegnazioni di sicurezza a livello di applicazione e di artifact in base alle nuove assegnazioni al gruppo.



Nota:

Tutti gli accessi utente identificati nel file di importazione devono essere presenti nel dominio identità; tutti i nomi di gruppo inclusi nel file devono essere presenti in Controllo accesso. Non è possibile creare un gruppo utilizzando questo processo di importazione.

È possibile creare solo nuove assegnazioni gruppo; non è possibile rimuovere le assegnazioni gruppo correnti degli utenti.

Nelle illustrazioni seguenti è visualizzato un possibile formato del file CSV di importazione:

```
User Login,Group
jdoe, Example_grp1
jane.doe@example.com, Example_grp2
```

```
User Login,First Name,Last Name,Email,Direct,Group
jdoe, John, Doe, jdoe@example.com, Yes, Example_grp1
jane.doe@example.com, Jane, Doe, jane.doe@example.com, No, Example_grp2
```

Questo formato è identico alla versione CSV del Report gruppo utenti. Se si utilizza questo formato, il processo di importazione ignorerà tutte le colonne tranne Accesso utente e Gruppo. Un modo semplice per creare un file di importazione è esportare il

Report gruppo utenti corrente e quindi modificarlo in base alle proprie esigenze. Fare riferimento a [Visualizzazione ed esportazione del Report gruppo utenti](#).

Per importare le assegnazioni di utenti al gruppo, precedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento alla sezione [Apertura di Controllo accesso](#).
2. Fare clic su **Report gruppo utenti**.
3. Fare clic su **Importa da CSV**.
4. Selezionare il file di importazione utilizzando **Sfoggia** in **Importa CSV assegnazione gruppo di utenti**.
5. Fare clic su **Importa**.
6. Fare clic su **Sì**.

Al termine del processo di importazione verrà visualizzata una finestra di dialogo di conferma nella quale sono indicati il numero totale di assegnazioni elaborate e il loro stato.



Assegnazione di un utente a molti gruppi

Gli utenti di Oracle Enterprise Performance Management Cloud possono essere membri di numerosi gruppi gestiti mediante Controllo accesso. Gli amministratori dei servizi o gli utenti con il ruolo applicazioneControllo accesso - Gestisci possono assegnare un utente a molti gruppi.





Nota:

In qualsiasi caso, un utente può essere membro di un massimo di 1000 gruppi direttamente o indirettamente.

1. Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
2. Fare clic su **Gestione utenti**.
3. Cercare l'utente da assegnare ai gruppi. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
Vengono elencati gli utenti che soddisfano i criteri di ricerca. Per impostazione predefinita, questo elenco è ordinato in base ai valori **Login utente**.
4. Fare clic su  (Azione) sulla riga dell'elenco di utenti, quindi selezionare **Modifica**.
Viene visualizzata la schermata **Modifica utente**, nella quale sono riportate le informazioni dettagliate sull'utente, inclusa l'appartenenza corrente ai gruppi (in **Gruppi assegnati**). In questa schermata è possibile modificare solo le assegnazioni dei gruppi.
5. Cercare i gruppi da assegnare all'utente. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
Vengono elencati i gruppi che soddisfano i criteri di ricerca. Per impostazione predefinita, questo elenco è ordinato in base ai valori **Nome gruppo**.
6. Completare un'azione tra le seguenti.
 - Per assegnare all'utente altri gruppi, selezionare uno o più gruppi in **Gruppi disponibili** e fare clic su  (**Sposta**) per spostare i gruppi selezionati in **Gruppi**

assegnati. In alternativa, fare clic su  (**Sposta tutto**) per spostare tutti i gruppi da **Gruppi disponibili** a **Gruppi assegnati**.

- Per rimuovere i gruppi assegnati all'utente, selezionare uno o più gruppi in **Gruppi assegnati** e fare clic su  (**Rimuovi**) per spostare i gruppi selezionati in **Gruppi disponibili**. In alternativa, fare clic su  (**Rimuovi tutto**) per spostare tutti i gruppi da **Gruppi assegnati** a **Gruppi disponibili**.

7. Fare clic su **Salva**.

8. Fare clic su **OK**.

Utilizzo della ricerca


La ricerca intelligente di artifact di utenti e gruppi funziona sempre nello stesso modo all'interno di Controllo accesso.

Per trovare specifici utenti, gruppi o ruoli, utilizzare come stringa di ricerca uno degli attributi utente (nome utente, nome, cognome o ID e-mail) oppure il nome del gruppo o il nome del ruolo. Non è necessario utilizzare caratteri jolly nelle stringhe di ricerca. Ad esempio, se si utilizza la stringa `st` per trovare i gruppi, la ricerca restituirà tutti i nomi dei gruppi che contengono la stringa `st`, come `TestGroup`, `Strategic_Planner`, `AnalystsGroup` e così via. Allo stesso modo, se si utilizza la stringa `jd` per trovare gli utenti, la ricerca restituirà l'elenco degli utenti il cui nome utente, nome, cognome o indirizzo e-mail contiene la stringa `jd`.


Nota:

Alcune schermate di Controllo accesso, ad esempio, **Assegna ruoli applicazione**, **Report assegnazioni ruoli** e **Report gruppo utenti**, offrono un'opzione di ricerca. Prima di avviare una ricerca, effettuare una selezione appropriata.

Per ricercare utenti, procedere come segue:

1. Accedere a una schermata, come ad esempio **Gestione utenti**, dove è disponibile la funzione di ricerca.
2. Nel campo di ricerca immettere una stringa parziale di un attributo utente (nome utente, nome, cognome o ID e-mail).
3. Fare clic su  (Cerca).
Nei risultati della ricerca vengono visualizzate tutte le proprietà disponibili per gli utenti che corrispondono ai criteri di ricerca. Per impostazione predefinita, questo elenco è ordinato in base ai valori **Login utente**.

Per ricercare gruppi, procedere come segue:

- Accedere a una schermata, come ad esempio **Gestione gruppi**, dove è disponibile la funzione di ricerca.
- Nel campo di ricerca immettere una stringa parziale del nome gruppo.
- Fare clic su  (Cerca).

Nei risultati della ricerca vengono visualizzati il nome e la descrizione dei gruppi che corrispondono ai criteri di ricerca. Per impostazione predefinita, questo elenco è ordinato in base ai valori **Nome gruppo**.

Create Group Save Close

* Name:

Description:

Groups **Users**

Available Users

First Name	Last Name	Email	User Login
John	Doe	john.doe@exam...	jdoe
Jane	Doe	jane.doe@exam...	jadoe31
Jane	Doe	jane.x.doe@exam	jadoe41

Assigned Users

First Name	Last Name	Email	User Login
No records were found.			

Per cercare gli utenti in base ai loro ruoli nel Report assegnazione ruoli, procedere come segue.

- Accedere alla scheda **Report assegnazione ruoli**.
- Selezionare **Utenti** o **Ruoli** nell'elenco a discesa per la ricerca.
- Nel campo della ricerca immettere una stringa da ricercare.
- Fare clic su (Cerca).
Nei risultati della ricerca vengono visualizzate tutte le informazioni disponibili per gli utenti assegnati ai ruoli che corrispondono ai criteri di ricerca. Per impostazione predefinita, questo elenco è ordinato in base ai valori **Login utente**.

2

Gestione dell'assegnazione dei ruoli a livello di applicazione

Related Topics

- [Panoramica dell'assegnazione dei ruoli applicazione](#)
- [Account Reconciliation](#)
- [Enterprise Profitability and Cost Management](#)
- [Planning, FreeForm, Financial Consolidation and Close e Tax Reporting](#)
- [Profitability and Cost Management](#)
- [Oracle Enterprise Data Management Cloud ed Enterprise Data Management](#)
- [Assegnazione di ruoli applicazione a un gruppo o a un utente](#)
- [Rimozione di ruoli a livello di applicazione assegnati a un gruppo o a un utente](#)

Panoramica dell'assegnazione dei ruoli applicazione

Controllo accesso consente di estendere le possibilità di accesso di un utente di Oracle Enterprise Performance Management Cloud oltre quelle concesse dal relativo ruolo predefinito assegnandogli ruoli a livello di applicazione (ruoli applicazione).

I ruoli predefiniti (Amministratore servizi, Utente avanzato, Utente e Visualizzatore) sono gerarchici, pertanto un ruolo più alto eredita i privilegi inclusi nei ruoli più bassi. Ad esempio, il ruolo Utente eredita l'accesso all'applicazione EPM Cloud autorizzato tramite il ruolo Visualizzatore. Analogamente, il ruolo Utente avanzato eredita i privilegi di accesso concessi dai ruoli Utente e Visualizzatore.

I ruoli applicazione consentono solo di migliorare i diritti di accesso degli utenti. Nessuno dei privilegi concessi da un ruolo predefinito può essere ridimensionato. Per gestire il processo di assegnazione di ruoli applicazione, è possibile utilizzare Controllo accesso ed eseguire i task descritti di seguito.

- Creare gruppi e aggiungere utenti EPM Cloud o altri gruppi come membri.
- Aggiungere o eliminare membri dei gruppi
- Assegnare ruoli applicazione a gruppi o utenti, inclusi se stessi
- Visualizzare un elenco di utenti membri di un gruppo

Mentre i diritti di accesso complessivi vengono controllati dai ruoli predefiniti, gli amministratori dei servizi o gli utenti con ruolo applicazione Controllo accesso - Gestisci possono concedere ruoli specifici dell'applicazione e autorizzazioni dati agli utenti e ai gruppi creati e gestiti in Controllo accesso.

Assegnare i ruoli applicazione appropriati agli utenti se questi devono eseguire funzioni non previste dai privilegi associati ai ruoli predefiniti di cui dispongono. Ad esempio, per impostazione predefinita solo gli amministratori servizi e gli utenti avanzati possono accedere a Integrazione dati. Per consentire agli utenti con il ruolo predefinito Utente o Visualizzatore

di partecipare al processo di integrazione, gli amministratori dei servizi devono assegnare loro i ruoli Integrazione dati (Integrazione dati - Crea).

Processi aziendali che supportano l'assegnazione di ruoli applicazione

I processi aziendali che supportano l'assegnazione di ruoli applicazione sono i seguenti.

- Planning, FreeForm, Financial Consolidation and Close e Tax Reporting
- Enterprise Profitability and Cost Management
- Oracle Enterprise Data Management Cloud
- Account Reconciliation

Altri processi aziendali, come Profitability and Cost Management e Narrative Reporting, non supportano l'assegnazione di ruoli applicazione.

Procedure consigliate per l'assegnazione di ruoli applicazione a un ruolo predefinito

La procedura consigliata prevede l'assegnazione del ruolo di livello inferiore più idoneo e la concessione di privilegi aggiuntivi, laddove necessario. Di seguito sono riportate alcune situazioni in cui si può decidere di concedere i ruoli applicazione a un utente che altrimenti non disporrebbe di tali privilegi specifici in base al ruolo predefinito associato.

- Aggiungere il ruolo applicazione **Preparatore** a un utente con ruolo Visualizzatore che deve preparare le riconciliazioni.
- Uno sviluppatore di report è impegnato solo nella progettazione dei report e non nelle altre funzionalità dell'applicazione. È pertanto possibile assegnare il ruolo Visualizzatore e quindi assegnare il ruolo applicazione **Gestione report**
- Consentire a un utente avanzato di gestire i tipi di avviso in modo che sia possibile assegnare il ruolo applicazione **Gestisci tipi di avviso**.

Note:

La concessione di privilegi è esclusivamente un processo additivo, nel senso che è possibile aggiungere privilegi ai privilegi associati al ruolo predefinito di un utente, ma non è possibile rimuovere i privilegi assegnati automaticamente a tale ruolo predefinito.

In caso di migrazione di applicazioni da un ambiente in locale a EPM Cloud, fare riferimento alla sezione "Mapping dei ruoli per la migrazione a EPM Cloud" nella guida *Administering Migration for Oracle Enterprise Performance Management Cloud (in lingua inglese)* per ulteriori informazioni su come assegnare i ruoli predefiniti agli utenti.

Utenti di EPM Cloud

È possibile creare e gestire gli utenti EPM Cloud nel dominio di Identity associato all'ambiente al quale appartiene il processo aziendale. Solo gli utenti assegnati ai ruoli predefiniti possono ottenere i ruoli a livello di applicazione per migliorare l'accesso di cui dispongono al fine di eseguire i task in un processo aziendale.

Informazioni sui ruoli predefiniti

Per informazioni sui ruoli predefiniti, fare riferimento agli argomenti indicati di seguito della *Guida introduttiva a Oracle Enterprise Performance Management Cloud per gli amministratori*.

- Informazioni sulla gestione di utenti e ruoli
- Introduzione ai ruoli predefiniti
- Ruoli predefiniti di Planning, Planning Modules e FreeForm
- Ruoli predefiniti di Financial Consolidation and Close
- Ruoli predefiniti di Tax Reporting
- Ruoli predefiniti di Profitability and Cost Management
- Ruoli predefiniti di Enterprise Profitability and Cost Management
- Ruoli predefiniti di Account Reconciliation
- Ruoli predefiniti di Enterprise Data Management
- Ruoli predefiniti di Strategic Workforce Planning
- Ruoli predefiniti di Narrative Reporting
- Ruoli predefiniti di Sales Planning

Risoluzione dei problemi

Fare riferimento alla sezione Risoluzione dei problemi di gestione utenti, ruoli e gruppi nella *Guida operativa di Oracle Enterprise Performance Management Cloud*.

Account Reconciliation

Related Topics

- [Ruoli applicazione](#)
- [Mapping dei ruoli predefiniti](#)

Ruoli applicazione

I ruoli elencati di seguito sono validi solo per **Riconciliazione conti**. Per impostazione predefinita, questi ruoli applicazione sono inclusi nei ruoli predefiniti. Fare riferimento alla sezione [Mapping dei ruoli predefiniti](#). I ruoli applicazione possono essere assegnati agli utenti che devono eseguire operazioni non previste dai privilegi associati ai loro ruoli predefiniti.

Tipi di avviso - Gestisci

Gestisce tutti i tipi di avviso per definire una procedura da seguire quando si verificano problemi specifici.

Annunci - Gestisci

Gestisce gli annunci che vengono visualizzati agli utenti nel Pannello di benvenuto. Possono indicare eventi futuri, come manutenzioni di sistema o l'esecuzione di job.

Audit - Visualizza

Fornisce l'accesso a tutti i dettagli dell'audit. Questo ruolo applicazione tuttavia non consente di visualizzare la finestra di dialogo Azioni riconciliazione relativa alle riconciliazioni che non rientrano nel relativo ambito di sicurezza.

Valute - Gestisci

Configura valute, tipi di tassi e gruppi di valute. Gli utenti con questo ruolo possono controllare i codici valuta che sono attivi nel sistema.

Dashboard - Gestisci

Consente di costruire e gestire dashboard customizzati. Gli utenti con questo ruolo possono:

- Configurare la conformità
- Aggiungere, modificare, duplicare ed eliminare
- Importare ed esportare

Integrazione dati - Amministratore

Esegue tutte le attività funzionali in Integrazione dati. Gli utenti con questo ruolo possono creare ed eseguire:

- integrazioni tra sistemi di origine e target;
- attività pipeline;
- estrazione e trasformazione di dati e metadati da origini in locale utilizzando l'agente di integrazione EPM.

Integrazione dati - Crea

Utilizza Integrazione dati per la creazione di mapping per integrare i dati tra sistemi di origine e target. Questo ruolo consente di definire regole dati con varie opzioni di runtime.

Integrazione dati - Drill-through

Esegue il drill-through nel sistema di origine dei dati.

Integrazione dati - Esegui

In Integrazione dati esegue regole dati con parametri di runtime e visualizza i log di esecuzione.

Caricamenti dati - Gestisci

Crea definizioni di caricamenti dati allo scopo di caricare dati tramite Integrazione dati e salvare i parametri di tali caricamenti dati. Visualizza lo stato più recente dei caricamenti di dati e monitora l'elaborazione delle richieste di modifica degli utenti.

Job - Visualizza

Visualizza i job di Riconciliazione dei conti e lo stato dei job.

Tipi di corrispondenza - Gestisci

Gli utenti con questo ruolo possono gestire i tipi di corrispondenze, gli attributi di adeguamento, gli attributi di supporto, le colonne giornale e gli attributi di gruppo.

Tipi di corrispondenza - Visualizza

Gli utenti con questo ruolo possono visualizzare i dettagli di tipi di corrispondenze, attributi di adeguamento, attributi di supporto e colonne giornale.

Organizzazioni - Gestisci

Assegna una struttura gerarchica delle unità organizzative ai profili e alle riconciliazioni.

Periodi - Gestisci

Gestisce le proprietà del periodo. Consente anche di impostare lo stato dei periodi, caricare i dati ed eseguire altre operazioni sui periodi esistenti.

Periodi - Visualizza

Gli utenti con questo ruolo possono visualizzare (accesso in sola lettura) il numero di periodi associati alle riconciliazioni e anche caricare i dati per il periodo.

Profili - Visualizza

Visualizza e riassegna i profili.

Profili e riconciliazioni - Gestisci

Gestisce i seguenti profili e riconciliazioni: Segmenti di profilo, Processo, Valutazione rischio, Frequenze, Tipo di conto, Profili scadenziario e Token integrazione globale. Oracle consiglia di verificare che l'ambito di sicurezza sia impostato in modo appropriato per questo utente.

Filtri e viste pubblici - Gestisci

I filtri consentono di controllare i record che sono visibili nelle viste elenco e nei report. È possibile applicare filtri a profili, riconciliazioni o attributi transazione di riconciliazione, inclusi attributi di sistema, saldi e dettagli dei saldi. Gli utenti con questo ruolo possono creare filtri e logiche complessi per determinare l'ordine di applicazione dei filtri.

Riconciliazione - Commentatore

Consente di visualizzare le riconciliazioni e aggiungere commenti alla riconciliazione o alle relative transazioni.

Riconciliazione - Preparatore

Gli utenti con questo ruolo preparano le riconciliazioni, assegnano i pannelli, importano i dati pre-mappati e aggiungono gli allegati per sottomettere, prendere in carico e rilasciare le riconciliazioni.

Riconciliazione - Revisore

Gli utenti con questo ruolo esaminano le riconciliazioni, assegnano pannelli e aggiungono allegati per approvare, rifiutare, prendere in carico e rilasciare le riconciliazioni.

Report - Gestisci

Configura le impostazioni dell'applicazione per visualizzare i report di riconciliazione.

Team - Gestisci

Gli utenti con questo ruolo possono aggiungere, modificare o rimuovere i team e gestirne i membri.

Utenti - Gestisci

Gli utenti con questo ruolo possono gestire i membri dei team.

Mapping dei ruoli predefiniti

Per un elenco delle attività Account Reconciliation che ogni ruolo applicazione può eseguire, fare riferimento alla sezione [Ruoli applicazione](#).

Tutti i ruoli applicazione Account Reconciliation sono mappati al ruolo predefinito Amministratore servizi. Gli utenti con questo ruolo possono eseguire tutte le attività a cui i singoli ruoli applicazione possono accedere. Di seguito sono elencati i ruoli applicazione Account Reconciliation mappati solo ad Amministratore servizi.

- Tipi di avviso - Gestisci
- Annunci - Gestisci
- Audit - Visualizza
- Valute - Gestisci
- Integrazione dati - Amministratore
- Integrazione dati - Crea
- Integrazione dati - Esegui
- Caricamenti dati - Gestisci
- Organizzazioni - Gestisci
- Periodi - Gestisci
- Filtri e viste pubblici - Gestisci
- Report - Gestisci

I ruoli applicazione Account Reconciliation sotto riportati sono mappati ai ruoli predefiniti diversi da Amministratore servizi.

Table 2-1 Ruoli applicazione inclusi nei ruoli predefiniti diversi da Amministratore servizi

Ruolo applicazione	Incluso in questi ruoli predefiniti
Dashboard - Gestisci	<ul style="list-style-type: none"> • Utente avanzato • Utente • Visualizzatore
Job - Visualizza	Utente avanzato
Periodi - Visualizza	Utente avanzato
Profili e riconciliazioni - Gestisci	Utente avanzato

Table 2-1 (Cont.) Ruoli applicazione inclusi nei ruoli predefiniti diversi da Amministratore servizi

Ruolo applicazione	Incluso in questi ruoli predefiniti
Profili - Visualizza	<ul style="list-style-type: none"> • Utente avanzato • Utente
Riconciliazione - Commentatore	<ul style="list-style-type: none"> • Utente avanzato • Utente
Riconciliazione - Preparatore	<ul style="list-style-type: none"> • Utente avanzato • Utente
Riconciliazione - Revisore	<ul style="list-style-type: none"> • Utente avanzato • Utente
Team - Gestisci	Utente avanzato
Utenti - Gestisci	Utente avanzato

Enterprise Profitability and Cost Management

Related Topics

- [Ruoli applicazione](#)
- [Mapping dei ruoli predefiniti](#)

Ruoli applicazione

I ruoli seguenti sono validi solo per Enterprise Profitability and Cost Management.

Per impostazione predefinita, questi ruoli applicazione sono inclusi nei ruoli predefiniti. Fare riferimento alla sezione [Mapping dei ruoli predefiniti](#). I ruoli applicazione possono essere assegnati agli utenti che devono eseguire operazioni non previste dai privilegi associati ai loro ruoli predefiniti.

Ad hoc - Crea

Crea, visualizza, modifica e salva le griglie ad hoc.

Ad hoc - Utente di sola lettura

Esegue tutte le funzioni ad hoc, ma non può scrivere nelle griglie ad hoc o caricare dati utilizzando Gestione dati.

Ad hoc - Utente

Visualizza e modifica le griglie ad hoc ed esegue operazioni ad hoc. Gli utenti ad hoc non possono salvare le griglie ad hoc.

Cronologia calcolo - Elimina

Elimina un'istanza selezionata di un calcolo completato dalla pagina Analisi calcolo. L'eliminazione della cronologia di calcolo non comporta l'eliminazione dei dati. Elimina semplicemente l'istanza registrata di un calcolo eseguito.

Calcolo - Esegui

Calcola un modello nella pagina Controllo calcolo.

Cronologia calcolo - Visualizza

Visualizza i calcoli completati dalla pagina Analisi calcolo.

Integrazione dati - Crea

Utilizza Integrazione dati per la creazione di mapping per integrare i dati tra sistemi di origine e target. Gli utenti possono definire regole dati con varie opzioni di runtime.

Integrazione dati - Drill-through

Esegue il drill-through nel sistema di origine dei dati.

Integrazione dati - Esegui

In Integrazione dati esegue regole dati con parametri di runtime e visualizza i log di esecuzione.

Modello - Crea

Crea un nuovo modello nella pagina Modellazione.

Modello - Elimina

Elimina un modello nella pagina Modellazione. L'eliminazione di un modello comporterà anche l'eliminazione di tutte le regole in esso contenute.

Modello - Visualizza

Visualizza i modelli e le relative regole associate nella pagina Designer.

Convalida modello - Esegui

Convalida i modelli nella pagina Convalida modello.

Dati POV - Cancella

Cancella i dati da un punto di vista nella pagina Controllo calcolo senza rimuovere il punto di vista.

Dati POV - Copia

Copia i dati da un punto di vista a un altro nella pagina Controllo calcolo.

POV - Crea

Crea un nuovo punto di vista nella pagina Controllo calcolo.

POV - Elimina

Elimina un punto di vista nella pagina Controllo calcolo. L'eliminazione di un punto di vista comporterà anche l'eliminazione dei dati associati, nonché della pagina con la cronologia di calcolo per il punto di vista in questione. Rimuove inoltre il punto di vista dalla pagina Controllo calcolo.

Stato POV - Modifica

Modifica lo stato di un punto di vista dalla finestra di dialogo Modifica punto di vista nella pagina Controllo calcolo. Gli stati disponibili per un punto di vista sono Bozza, Pubblicato e Archiviato.

Curva profitto - Crea

Crea le curve del profitto nella scheda Curve del profitto del cluster Intelligence.

Curva profitto - Modifica

Modifica le curve del profitto nella scheda Curve del profitto del cluster Intelligence.

Curva profitto - Esegui

Esegue le curve del profitto nella scheda Curve del profitto del cluster Intelligence.

Regola - Crea/Modifica

Crea o modifica una regola di allocazione, una regola di calcolo customizzata o un set di regole nella pagina Designer.

Regola - Elimina

Elimina una regola di allocazione, una regola di calcolo customizzata o un set di regole nella pagina Designer.

Bilanciamento regola - Esegui

Visualizza il report Bilanciamento regola per mostrare l'impatto di ciascuna regola.

Regole - Modifica di massa

Porta alla scheda Modifica di massa nella pagina Designer e consente di apportare modifiche a più regole contemporaneamente.

Elenco task - Gestisci accesso

Assegna i task ad altri utenti.

Traccia allocazione - Esegui

Traccia gli importi di allocazione nella scheda Traccia allocazioni del cluster Intelligence.

Mapping dei ruoli predefiniti

Per un elenco delle attività Enterprise Profitability and Cost Management che ogni ruolo applicazione può eseguire, fare riferimento alla sezione [Ruoli applicazione](#).

Tutti i ruoli applicazione sono mappati al ruolo predefinito Amministratore servizi. Gli utenti con questo ruolo possono eseguire tutte le attività a cui i singoli ruoli applicazione possono accedere. Di seguito sono elencati i ruoli applicazione Enterprise Profitability and Cost Management mappati solo ad Amministratore servizi.

- Ad hoc - Utente di sola lettura
- Modello - Elimina

- POV - Elimina
- Stato POV - Modifica

I ruoli applicazione Enterprise Profitability and Cost Management sotto riportati sono mappati ai ruoli predefiniti diversi da Amministratore servizi.

Table 2-2 Ruoli applicazione inclusi nei ruoli predefiniti diversi da Amministratore servizi

Ruolo applicazione	Incluso in questi ruoli predefiniti
Ad hoc - Crea	Utente avanzato
Ad hoc - Utente	<ul style="list-style-type: none"> • Utente avanzato • Utente
Cronologia calcolo - Elimina	<ul style="list-style-type: none"> • Utente avanzato • Utente
Calcolo - Esegui	Utente avanzato
Cronologia calcolo - Visualizza	<ul style="list-style-type: none"> • Utente avanzato • Utente
Integrazione dati - Crea	Utente avanzato
Integrazione dati - Drill-through	<ul style="list-style-type: none"> • Utente avanzato • Utente
Integrazione dati - Esegui	Utente avanzato
Modello - Crea	Utente avanzato
Modello - Visualizza	<ul style="list-style-type: none"> • Utente avanzato • Utente • Visualizzatore
Convalida modello - Esegui	<ul style="list-style-type: none"> • Utente avanzato • Utente
Dati POV - Cancella	Utente avanzato
Dati POV - Copia	Utente avanzato
POV - Crea	Utente avanzato
Curva profitto - Crea	Utente avanzato
Curva profitto - Modifica	Utente avanzato
Curva profitto - Esegui	<ul style="list-style-type: none"> • Utente avanzato • Utente • Visualizzatore
Regola - Crea/Modifica	<ul style="list-style-type: none"> • Utente avanzato • Utente
Regola - Elimina	<ul style="list-style-type: none"> • Utente avanzato • Utente
Bilanciamento regola - Esegui	<ul style="list-style-type: none"> • Utente avanzato • Utente
Regole - Modifica di massa	<ul style="list-style-type: none"> • Utente avanzato • Utente
Elenco task - Gestisci accesso	Utente avanzato
Traccia allocazione - Esegui	<ul style="list-style-type: none"> • Utente avanzato • Utente • Visualizzatore

Planning, FreeForm, Financial Consolidation and Close e Tax Reporting



Note:

Planning include tipi di applicazioni customizzate, FreeForm , Planning Modules, Strategic Workforce Planning e Sales Planning.

In questa sezione vengono trattati i ruoli applicazione indicati di seguito.

- [Ruoli della piattaforma EPM Cloud](#) (I ruoli di approvazione non sono applicabili a Financial Consolidation and Close e FreeForm)
- [Ruoli di Integrazione dati](#)
- [Ruoli correlati al giornale di consolidamento](#) (applicabile solo a Financial Consolidation and Close)
- [Ruoli Task Manager](#) (non applicabile a FreeForm)

Per impostazione predefinita, questi ruoli applicazione sono inclusi nei ruoli predefiniti. Fare riferimento alla sezione [Mapping dei ruoli predefiniti](#).

Ruoli della piattaforma EPM Cloud



Note:

I ruoli di approvazione non sono applicabili a Financial Consolidation and Close e FreeForm.

Ad hoc - Crea

Crea, visualizza, modifica e salva le griglie ad hoc.

Ad hoc - Utente di sola lettura

Esegue tutte le funzioni ad hoc, ma non può scrivere nelle griglie ad hoc o caricare dati utilizzando Gestione dati.

Ad hoc - Utente

Visualizza e modifica le griglie ad hoc ed esegue operazioni ad hoc. Gli utenti ad hoc non possono salvare le griglie ad hoc.

Applicazione - Allocazione di massa

Esegue le regole di allocazione di massa all'interno delle griglie di form.

Approvazioni - Amministra

Risolve i problemi di approvazione assumendo manualmente la proprietà del processo. Comprende i ruoli Assegnatario proprietà approvazioni, Designer processo approvazioni e Supervisore approvazioni.

Di solito, questo ruolo viene assegnato a utenti aziendali responsabili di una regione che devono controllare il processo delle approvazioni per la regione, ma che non devono per forza avere il ruolo Amministratore servizi. Possono eseguire i task seguenti:

- Controllare il processo delle approvazioni.
- Eseguire azioni sulle unità di Planning per le quali dispongono di accesso in scrittura.
- Assegnare proprietari e revisori per l'organizzazione di cui sono responsabili.
- Modificare la dimensione secondaria o aggiornare le regole di convalida.

Approvazioni - Assegna proprietà

Esegue i task seguenti per qualsiasi membro nella gerarchia dell'unità di pianificazione per la quale l'utente dispone dell'accesso in scrittura.

- Assegnare proprietari.
- Assegnare revisori.
- Specificare gli utenti a cui inviare notifica.

Approvazioni - Progetta processo

Include il ruolo Assegnatario proprietà approvazioni. Inoltre, esegue i task seguenti per qualsiasi membro nella gerarchia dell'unità di pianificazione per la quale dispone dell'accesso in scrittura.

- Modificare dimensioni secondarie e membri delle entità per le quali l'utente dispone dell'accesso in scrittura.
- Modificare l'assegnazione di scenario e versione per una gerarchia di unità di pianificazione.
- Modificare le regole di convalida dei dati dei form dati per i quali l'utente dispone dell'accesso.

Approvazioni - Supervisiona

Esegue i task seguenti per qualsiasi membro nella gerarchia dell'unità di pianificazione per la quale l'utente dispone dell'accesso in scrittura, anche se non è il proprietario dell'unità di pianificazione. Questo utente non può modificare i dati nelle unità di pianificazione di cui non è proprietario.

- Arrestare e avviare un'unità di pianificazione.
- Eseguire qualsiasi azione su un'unità di pianificazione.

Elenco task - Gestisci accesso

Assegna i task ad altri utenti.

Ruoli di Integrazione dati

Integrazione dati - Crea

Utilizza Integrazione dati per la creazione di mapping per integrare i dati tra sistemi di origine e target. Gli utenti possono definire regole dati con varie opzioni di runtime.

Integrazione dati - Drill-through

Esegue il drill-through nel sistema di origine dei dati.

Integrazione dati - Esegui

In Integrazione dati esegue regole dati con parametri di runtime e visualizza i log di esecuzione.

Ruoli correlati al giornale di consolidamento



Note:

I ruoli correlati al giornale di consolidamento sono applicabili solo a Financial Consolidation and Close.

Giornali di consolidamento - Approva

Approvare un giornale di consolidamento sottomesso per l'approvazione o rifiutare un giornale sottomesso.

Giornali di consolidamento - Contabilizzazione automatica dopo l'approvazione

Consente la contabilizzazione automatica di un giornale di consolidamento dopo che è stato approvato dall'approvatore. L'utente che ha approvato il giornale sarà anche l'utente che lo contabilizza.

Giornali di consolidamento - Crea

Creare, modificare o eliminare giornali di consolidamento e template di giornali di consolidamento.

Giornali di consolidamento - Gestione periodi

Aprire i periodi di tempo per i giornali di consolidamento o chiudere i periodi di tempo del giornale. Se nel periodo sono presenti giornali approvati o giornali con storno automatico non contabilizzati, non è possibile chiuderli. Se si seleziona un periodo che contiene giornali in stato Elaborazione in corso o Sottomesso, viene visualizzato un messaggio di avvertenza che segnala che sono stati trovati giornali non contabilizzati per il periodo, che però può essere chiuso.

Giornali di consolidamento - Contabilizza

Contabilizzare un giornale di consolidamento che è stato completato o sottomesso e approvato. È necessario innanzitutto aprire il periodo di tempo per ogni scenario in cui devono essere contabilizzati giornali di consolidamento.

Giornali di consolidamento - Sottometti

Sottomettere un giornale di consolidamento per l'approvazione o rifiutare un giornale di consolidamento con stato Completato.

Giornali di consolidamento - Annulla contabilizzazione

Annullare la contabilizzazione di un giornale di consolidamento. È necessario disporre dell'accesso in scrittura per i membri del giornale.

Ruoli Task Manager



Note:

I ruoli basati su Task Manager non sono validi per FreeForm.

Task Manager - Dashboard operativi - Gestisci

Configura il dashboard

Task Manager - Report customizzati - Gestisci

Progetta i report customizzati

Task Manager - Approvatore

Idoneo come approvatore per i task da Task Manager

Task Manager - Assegnatario

Idoneo come assegnatario per i task da Task Manager

Task Manager - Artifact - Gestisci

Gestisce tutti gli artifact di Task Manager, ad esempio avvisi, valute e organizzazione

Task Manager - Servizi e impostazioni di sistema - Gestisci

Definisce i servizi e le impostazioni di sistema per un'applicazione

Task Manager - Viste e filtri pubblici - Gestisci

Pubblica i filtri e le viste per renderli accessibili a tutti

Task Manager - Task - Gestisci

Progetta e gestisce i task, i template e le programmazioni

Task Manager - Utenti e team - Gestisci

Gestisce gli utenti e i team

Task Manager - Audit - Visualizza

Visualizza le informazioni della cronologia di audit

Mapping dei ruoli predefiniti

A meno che non specificato diversamente, tutti i ruoli applicazione della piattaforma EPM Cloud sono mappati sul ruolo predefinito Amministratore servizi. Gli utenti con questo ruolo possono eseguire tutte le attività a cui i singoli ruoli applicazione possono accedere. Di seguito sono elencati i ruoli applicazione mappati solo sul ruolo Amministratore servizi.

- Ad hoc - Utente di sola lettura
- Approvazioni - Progetta processo
- Task Manager - Dashboard operativi - Gestisci
- Task Manager - Report customizzati - Gestisci
- Task Manager - Artifact - Gestisci
- Task Manager - Servizi e impostazioni di sistema - Gestisci
- Task Manager - Audit - Visualizza

I **ruoli correlati al giornale di consolidamento** non sono associati ad alcun ruolo predefinito. Questi ruoli dell'applicazione devono essere assegnati separatamente a ciascun utente o gruppo. Se questi ruoli non vengono assegnati, l'utente non può eseguire alcuna attività correlata al giornale di consolidamento oltre alla visualizzazione dei giornali.

I ruoli applicazione elencati di seguito sono mappati su ruoli predefiniti diversi da Amministratore servizi.

Table 2-3 Ruoli applicazione inclusi nei ruoli predefiniti diversi da Amministratore servizi

Ruolo applicazione	Inclusi in questi ruoli predefiniti
Ad hoc - Crea	Utente avanzato
Ad hoc - Utente	Utente
Approvazioni - Assegna proprietà	Utente avanzato
Approvazioni - Supervisiona	Utente avanzato
Integrazione dati - Crea	Utente avanzato
Integrazione dati - Drill-through	<ul style="list-style-type: none"> • Utente avanzato • Utente
Integrazione dati - Esegui	Utente avanzato
Elenco task - Gestisci accesso	Utente avanzato
Task Manager - Approvatore	<ul style="list-style-type: none"> • Utente avanzato • Utente
Task Manager - Assegnatario	<ul style="list-style-type: none"> • Utente avanzato • Utente
Task Manager - Task - Gestisci	Utente avanzato
Task Manager - Utenti e team - Gestisci	Utente avanzato
Task Manager - Viste e filtri pubblici - Gestisci	Utente avanzato

Profitability and Cost Management

Related Topics

- [Ruoli applicazione](#)
- [Mapping dei ruoli predefiniti](#)

Ruoli applicazione

Il ruolo applicazione seguente è valido solo per Profitability and Cost Management.

Integrazione dati - Amministratore

Esegue tutte le attività funzionali in Integrazione dati. Gli utenti con questo ruolo possono creare ed eseguire:

- integrazioni tra sistemi di origine e target;
- attività pipeline;
- estrazione e trasformazione di dati e metadati da origini in locale utilizzando l'agente di integrazione EPM.

Migrazioni - Amministratore

Utilizza Migrazione per esportare e importare snapshot e artifact dall'applicazione. Gli utenti con questo ruolo possono creare applicazioni eseguendo la migrazione degli snapshot ed eliminare le applicazioni che hanno creato.

Gli utenti con questo ruolo non possono clonare gli ambienti.

Mapping dei ruoli predefiniti

Per un elenco delle attività Profitability and Cost Management che ogni ruolo applicazione può eseguire, fare riferimento alla sezione [Ruoli applicazione](#).

Tutti i ruoli applicazione sono mappati al ruolo predefinito Amministratore servizi. Gli utenti con questo ruolo possono eseguire tutte le attività a cui i singoli ruoli applicazione possono accedere.

Oracle Enterprise Data Management Cloud ed Enterprise Data Management

Related Topics

- [Ruoli applicazione](#)
- [Mapping dei ruoli predefiniti](#)

Ruoli applicazione

I seguenti ruoli si applicano solo a Oracle Enterprise Data Management Cloud e al processo aziendale Enterprise Data Management. Per impostazione predefinita, questi ruoli applicazione sono inclusi nei ruoli predefiniti. Fare riferimento alla sezione

Mapping dei ruoli predefiniti. I ruoli applicazione possono essere assegnati agli utenti che devono eseguire operazioni non previste dai privilegi associati ai loro ruoli predefiniti. Non è possibile migrare ruoli applicativi da in locale a Oracle Enterprise Data Management Cloud.

Controllo accesso - Gestisci

Gli utenti con questo ruolo possono gestire gruppi, assegnare ruoli applicazione a un gruppo o a un utente. Possono inoltre generare report sulla sicurezza degli utenti.

Applicazione - Crea

Registra le applicazioni in Oracle Enterprise Data Management Cloud. All'utente che registra un'applicazione viene assegnata l'autorizzazione Proprietario applicazione. All'utente viene inoltre assegnato il ruolo di proprietario della vista predefinita dell'applicazione.

Audit

Visualizza le informazioni relative all'audit, ad esempio la cronologia delle transazioni e le richieste di modifica dei dati in Oracle Enterprise Data Management Cloud.

Migrazioni - Amministra

Utilizza Migrazione per esportare e importare snapshot e artifact dall'applicazione. Gli utenti con questo ruolo possono creare applicazioni eseguendo la migrazione degli snapshot ed eliminare le applicazioni che hanno creato.

Gli utenti con questo ruolo non possono clonare gli ambienti.

Viste - Crea

Crea viste in un'applicazione Oracle Enterprise Data Management Cloud. All'utente che crea una vista viene assegnata l'autorizzazione Proprietario vista per la vista creata.

Mapping dei ruoli predefiniti

Per un elenco delle attività di Oracle Enterprise Data Management Cloud che ciascun ruolo applicazione può eseguire, fare riferimento alla sezione [Ruoli applicazione](#). Tutti i ruoli applicazione sono mappati al ruolo predefinito Amministratore servizi. Gli utenti con questo ruolo possono eseguire tutte le attività a cui i singoli ruoli applicazione possono accedere.

Di seguito sono elencati i ruoli applicazione Oracle Enterprise Data Management Cloud mappati solo ad Amministratore servizi.

- Controllo accesso - Gestisci
- Applicazione - Crea
- Audit
- Migrazioni - Amministra
- Viste - Crea

Assegnazione di ruoli applicazione a un gruppo o a un utente


Durante questo processo, gli amministratori dei servizi o gli utenti con ruolo applicazione Controllo accesso - Gestisci possono assegnare o annullare l'assegnazione di ruoli applicazione a gruppi e utenti a cui è assegnato un ruolo predefinito. Possono inoltre assegnare a se stessi i ruoli applicazione.

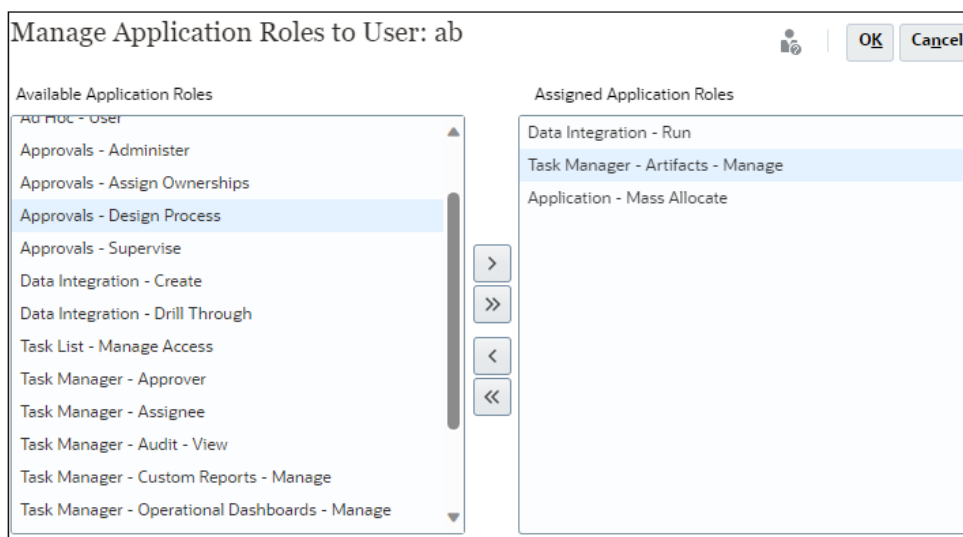
Per informazioni sui gruppi e sugli utenti assegnati a gruppi, fare riferimento alla sezione [Gestione di gruppi](#).

Per assegnare o annullare l'assegnazione di ruoli applicazione a un gruppo o a un utente, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento alla sezione [Apertura di Controllo accesso](#).
2. Fare clic sulla scheda **Gestisci ruoli applicazione**.
3. Individuare un utente o un gruppo. Nell'elenco a discesa, selezionare **Utenti** o **Gruppi**. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).

Vengono elencati gli utenti o i gruppi che soddisfano i criteri di ricerca. Per impostazione predefinita, l'elenco è ordinato in base ai valori **Login utente** e quindi in base ai valori **Nome gruppo** (per le ricerche di gruppi).

4. Fare clic su  (**Azioni**) per l'utente o il gruppo, quindi selezionare **Gestione ruoli**.
5. Per assegnare un ruolo applicazione all'utente o al gruppo, effettuare una selezione dall'elenco **Ruoli applicazione disponibili**, quindi fare clic sul pulsante freccia a destra.

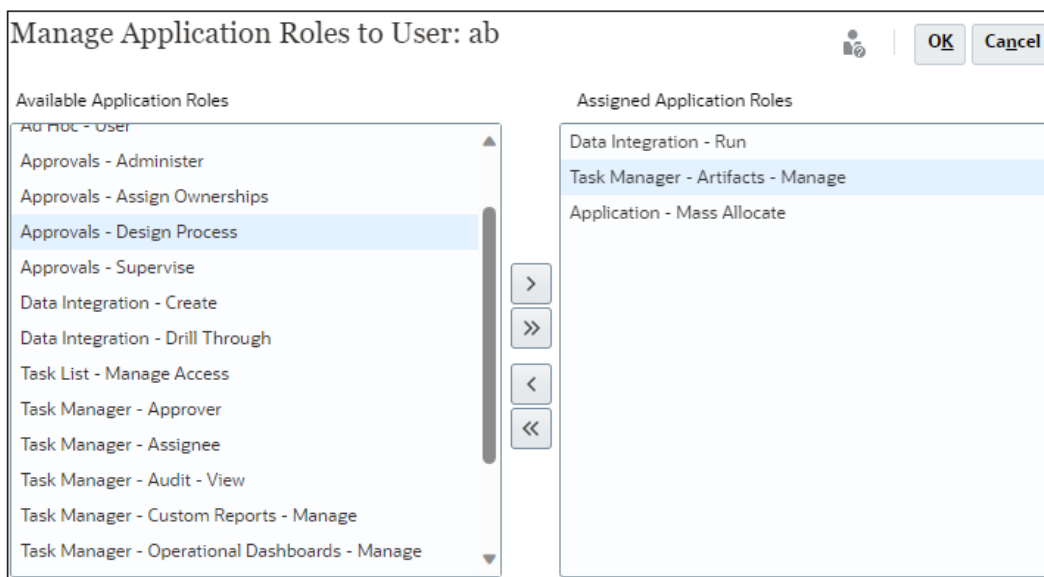


Per informazioni sui ruoli applicazione validi per ciascun processo aziendale, fare riferimento all'argomento appropriato.

- [Ruoli applicazione Account Reconciliation](#)
- [Ruoli applicazione Enterprise Profitability and Cost Management](#)
- [Planning, FreeForm, Financial Consolidation and Close e Tax Reporting Ruoli applicazione](#)
- [Ruoli dell'applicazione Oracle Enterprise Data Management Cloud](#)

Altri processi aziendali, come Profitability and Cost Management e Narrative Reporting, non supportano l'assegnazione di ruoli applicazione.

- Se si desidera annullare l'assegnazione di un ruolo applicazione, effettuare una selezione dall'elenco **Ruoli applicazione assegnati**, quindi fare clic sul pulsante freccia a sinistra.



- Fare clic su **OK** per completare l'assegnazione del ruolo applicazione per l'utente o il gruppo.
- Fare di nuovo clic su **OK** per tornare alla scheda **Gestisci ruoli applicazione**.


Rimozione di ruoli a livello di applicazione assegnati a un gruppo o a un utente

Durante questo processo, gli amministratori dei servizi o gli utenti con ruolo applicazione Controllo accesso - Gestisci possono rimuovere tutti i ruoli applicazione assegnati al gruppo o all'utente. La rimozione di un'assegnazione ruolo a livello di applicazione non influisce sui ruoli predefiniti dell'utente.

Per rimuovere i ruoli a livello di applicazione di un gruppo o di un utente, procedere come segue.

- Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
- Fare clic su **Assegna ruoli applicazione**.
- Individuare un utente o un gruppo. Nell'elenco a discesa, selezionare **Utenti** o **Gruppi**. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).

Vengono elencati gli utenti o i gruppi che soddisfano i criteri di ricerca. Per impostazione predefinita, l'elenco è ordinato in base ai valori **Login utente** e quindi in base ai valori **Nome gruppo** (per le ricerche di gruppi).

- Fare clic su  (Azioni) per l'utente o il gruppo, quindi selezionare **Annulla assegnazione ruoli**.
- Fare clic su **Sì**.
- Fare clic su **OK**.

3

Generazione di report

Gli amministratori dei servizi o gli utenti con ruolo applicazione Controllo accesso - Gestisci possono generare questi report per analizzare e gestire le assegnazioni di ruolo:

- [Generazione di un Report assegnazioni ruoli per un utente o un gruppo](#)
- [Visualizzazione del Report assegnazioni ruoli per l'ambiente](#)
- [Visualizzazione del Report accesso utenti](#)
- [Visualizzazione ed esportazione del Report gruppo utenti](#)

L'ora di generazione indicata nei report si basa sul formato del fuso orario del browser (clock di sistema locale).

Informazioni sulla versione CSV del report

È possibile esportare un report in modo da creare una versione CSV (Comma Separated Vale, valori separati da virgole) del report. Oltre al numero di utenti assegnati ai ruoli predefiniti, la versione CSV del report fornisce le informazioni riportate di seguito.

- Ruoli predefiniti a cui ciascun utente è assegnato. Ogni ruolo predefinito assegnato a un utente è indicato in una riga separata. I ruoli applicazione inclusi nei ruoli predefiniti non compaiono nell'elenco.
- Ruoli applicazione a cui un utente è assegnato, direttamente o attraverso un gruppo. Ogni ruolo applicazione assegnato a un utente appare in una riga separata.
- I gruppi a cui sono assegnati gli utenti non sono elencati se ai gruppi non è assegnato alcun ruolo.
- Solo le informazioni della vista corrente del report verranno esportate in formato CSV. Ad esempio, se al report si applica un filtro per visualizzare le assegnazioni di ruolo di un utente specifico, il file CSV esportato conterrà solo le assegnazioni di quell'utente.

Risoluzione dei problemi

Fare riferimento alla sezione Risoluzione dei problemi relativi ai report nella *Guida operativa di Oracle Enterprise Performance Management Cloud*.

Generazione di un Report assegnazioni ruoli per un utente o un gruppo


Il report assegnazioni ruoli consente di tenere traccia dell'accesso degli utenti ai fini del reporting per la conformità.

Questo report mostra tutti gli utenti attivi a cui è stato assegnato un ruolo predefinito. Gli utenti disattivati non vengono inclusi in questo report. I gruppi a cui un utente appartiene non sono riportati se non sono utilizzati per assegnare ruoli applicazione all'utente stesso. Gli amministratori dei servizi o gli utenti con ruolo applicazione Gestione controllo accesso possono accedere al Report assegnazione ruoli per rivedere i ruoli predefiniti assegnati e i ruoli applicazione di un utente o gruppo.

Per generare un Report assegnazioni ruoli per un utente o un gruppo, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
2. Fare clic sulla scheda **Gestisci ruoli applicazione**.
3. Individuare un utente o un gruppo. Nell'elenco a discesa, selezionare **Utenti o Gruppi**. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).

Vengono elencati gli utenti o i gruppi che soddisfano i criteri di ricerca. Per impostazione predefinita, il report è ordinato in base ai valori **Accesso utente** e quindi in base ai valori **Nomi gruppo** (per le ricerche di gruppi).

4. Fare clic su  per l'utente o il gruppo, quindi selezionare **Report assegnazioni ruoli**.
5. **Opzionale:** fare clic su **Esporta in formato CSV** per esportare il report in un file CSV.

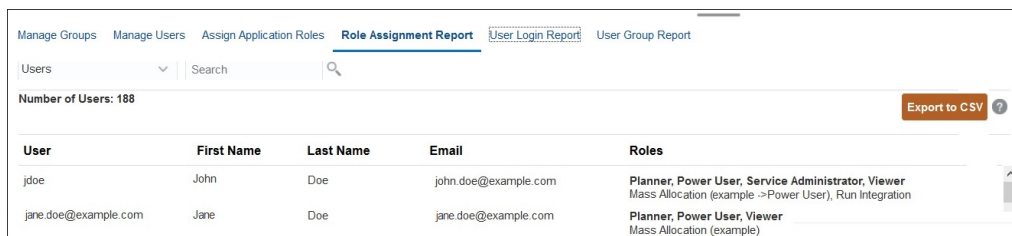
Visualizzazione del Report assegnazioni ruoli per l'ambiente

Gli amministratori dei servizi o gli utenti con ruolo applicazione Controllo accesso - Gestisci possono utilizzare il Report assegnazioni ruoli per esaminare l'accesso, assegnato tramite i ruoli predefiniti (in grassetto) e i ruoli a livello di applicazione, di tutti gli utenti. Questo report mostra tutti gli utenti attivi a cui è stato assegnato un ruolo predefinito. Gli utenti disattivati non vengono inclusi in questo report.

I ruoli ereditati, con le informazioni sull'eredità, vengono visualizzati in una riga apposita per ogni utente. Ad esempio, si supponga che all'utente John Doe venga assegnato il ruolo predefinito `User` e che `User` sia un membro del gruppo `example` al quale è assegnato il ruolo `Approvals - Administrator` dell'applicazione `Planning`. In questo scenario, all'interno delle informazioni sull'assegnazione di ruoli per John Doe, il Report assegnazioni ruoli visualizza quanto segue:

`Approvals - Administrator (example->User)`.

In un ambiente OCI (Gen 2), se un ruolo predefinito è assegnato a un gruppo IDCS, nel Report assegnazioni ruoli tale ruolo predefinito risulterà direttamente assegnato a tutti gli utenti del gruppo. Non sono riportati i ruoli dell'applicazione inclusi nei ruoli predefiniti o i ruoli del componente dei ruoli dell'applicazione assegnati all'utente. Per ottenere un report che mostri questi dettagli, è possibile generare la versione classica del report mediante il comando `provisionReport` di EPM Automate.



User	First Name	Last Name	Email	Roles
jdoe	John	Doe	john.doe@example.com	Planner, Power User, Service Administrator, Viewer Mass Allocation (example ->Power User), Run Integration
jane.doe@example.com	Jane	Doe	jane.doe@example.com	Planner, Power User, Viewer Mass Allocation (example)

È possibile esportare il Report assegnazioni ruoli come file CSV, che può essere aperto con un programma quale Microsoft Excel o salvato sul computer in uso. Il Report assegnazioni ruoli in formato CSV utilizza una riga per ogni assegnazione di ruolo.

	A	B	C	D	E	F
1	User Login	First Name	Last Name	Email	Role	Granted through Group
2	Jdoe	John	Doe	jdoe@example.com	Planner	
3	jdoe	John	Doe	jdoe@example.com	Power User	
4	Jdoe	John	Doe	jdoe@example.com	Service Administrator	
5	jdoe	John	Doe	jdoe@example.com	Viewer	
6	Jdoe	John	Doe	jdoe@example.com	Mass Allocation	example->Power User
7	jdoe	John	Doe	jdoe@example.com	Run Integration	
8	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Planner	
9	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Power User	
10	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Viewer	
11	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Mass Allocation	example

Per aprire il Report assegnazioni ruoli, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento alla sezione [Apertura di Controllo accesso](#).
2. Fare clic su **Report assegnazioni ruoli**.
Verrà visualizzato il Report assegnazioni ruoli.
3. **Facoltativo:** applicare il filtro al report per visualizzare gli elementi indicati di seguito.
 - Assegnazioni ruoli di un utente specifico. Selezionare **Utenti** nell'elenco a discesa, quindi immettere una stringa di ricerca parziale. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
 - Utenti assegnati a un ruolo specifico. Selezionare **Ruoli** nell'elenco a discesa, quindi immettere il nome parziale del ruolo. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).

 **Nota:**

È possibile assegnare gli utenti a molti ruoli. In tali casi, nel report vengono elencati tutti i ruoli dell'utente anche se il filtro è per un ruolo specifico.

Viene visualizzato il Report assegnazioni ruoli. Per impostazione predefinita, il report è ordinato in base ai valori **Login utente** e quindi in base ai ruoli applicazione in **Ruoli** (per le ricerche per ruolo). I ruoli predefiniti sono visualizzati in grassetto, a differenza dei ruoli applicazione.

4. **Opzionale:** fare clic su **Esporta in formato CSV** per esportare il report in un file CSV. Si noti che in formato CSV vengono esportate solo le informazioni del report correntemente visualizzato.

Visualizzazione del Report accesso utenti

Per impostazione predefinita, il Report accesso utenti contiene informazioni sugli utenti che hanno effettuato l'accesso all'ambiente nelle ultime 24 ore. Il report elenca l'indirizzo IP del computer da cui l'utente ha effettuato l'accesso e la data e l'ora (UTC) in cui l'utente ha effettuato l'accesso all'ambiente.

Gli amministratori dei servizi o gli utenti con ruolo Controllo accesso - Gestisci possono generare di nuovo questo report per un intervallo di date customizzato oppure per gli ultimi 30 giorni, gli ultimi 90 giorni e gli ultimi 120 giorni. Possono inoltre applicare un filtro al report per visualizzare solo le informazioni di utenti specifici utilizzando come stringa di ricerca una stringa parziale del nome, del cognome o dell'ID utente dell'utente.

 **Nota:**

In Oracle Enterprise Performance Management Cloud la cronologia di audit degli accessi utente viene conservata solo per gli ultimi 120 giorni.

Per generare un report sugli accessi utente, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
2. Fare clic su **Report attività accesso utenti**.
Viene visualizzato un report in cui sono elencati tutti gli utenti che hanno effettuato l'accesso all'ambiente nell'ultimo giorno.
3. Selezionare un periodo, ad esempio Ultimo giorno, Ultimi 30 giorni, Ultimi 90 giorni o Ultimi 120 giorni, in base al quale generare il report. Per specificare un intervallo di date customizzato, selezionare **Intervallo date**, quindi selezionare una data di inizio e una di fine.
4. **Facoltativo:** selezionare gli utenti da includere nel report. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).
Viene visualizzato il report Login utente. Per impostazione predefinita, il report è ordinato in base ai valori **Data e ora accesso**.
5. **Facoltativo:** fare clic su **Esporta in formato CSV** per esportare il report visualizzato in un file CSV.
6. Fare clic su **Annulla** per chiudere il report.

Visualizzazione ed esportazione del Report gruppo utenti

Nel Report gruppo utenti è indicata l'appartenenza, diretta o indiretta, degli utenti assegnati ai gruppi in Controllo accesso. Gli amministratori dei servizi o gli utenti con ruolo Controllo accesso - Gestisci possono generare questo report.

Gli utenti che sono assegnati a un gruppo, ne sono automaticamente membri diretti; sono considerati membri indiretti se sono assegnati a un gruppo che è un figlio di un altro gruppo. Per ogni utente assegnato a un gruppo, nel report sono fornite informazioni quali ID di accesso, nome e cognome, ID e-mail e un elenco separato da virgole dei gruppi ai quali l'utente è assegnato direttamente o indirettamente. I gruppi diretti sono visualizzati in grassetto, a differenza di quelli non diretti. Nella versione CSV del report è indicato se l'utente è assegnato direttamente o indirettamente a un gruppo tramite la dicitura Sì o No.

 **Nota:**

Questo report non è applicabile ad Account Reconciliation e Narrative Reporting.

Per rigenerare il Report gruppo utenti, procedere come segue.

1. Aprire **Controllo accesso**. Fare riferimento a [Apertura di Controllo accesso](#).
2. Fare clic su **Report gruppo utenti**.

3. **Facoltativo:** applicare il filtro al report. Nell'elenco a discesa, selezionare **Utenti o Gruppi**. Per istruzioni sull'utilizzo della funzione di ricerca, fare riferimento alla sezione [Utilizzo della ricerca](#).

Viene visualizzato il report relativo ai gruppi di utenti. Per impostazione predefinita, il report è ordinato in base ai valori **Login utente**.

4. **Opzionale:** fare clic su **Esporta in formato CSV** per esportare il report in un file CSV.
5. Fare clic su **Annulla** per chiudere il report.